REMARKS

I. Objection to the Title

The examiner objected to the title. The title has been amended.

II. Rejection of Claims 3-4 under 35 U.S.C. 112

Claims 3-4 were previously rejected under 35 U.S.C. 112. Claims 3-4 have been amended.

III. Rejection of claims 1-8 under 35 U.S.C. 103(a) based on Schneier

Claims 1-8 have been rejected under 35 U.S.C. 103(a) based on Schneier. These rejections are respectfully traversed as will be explained. However, claims 1, 6, and 8 have been amended to more clearly define the present invention.

Claim 1 specifies:

1. A method comprising the steps of:
encrypting a data message m using a primary transmitter secret key z to form a quantity E;
preparing a quadruplet (a_{new}, b_{new},s_{new}, E) where:
$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$ modulo p;
s_{new} = signature $_c(a_{new},b_{new},E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;
wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};
verifying the signature s_{new};
decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;
using the primary transmitter secret key z to decrypt the quantity E and thereby

obtaining the message m.

In the present application, in one or more embodiments, an encryption is peformed using a random number "c" and a signature is performed using the same random number "c". (Present application, paragraph 2, pg. 8). The prior art does not show these limitations, at least in combination. The Schneier reference in fact, teaches away from using the same random number for both an encryption process and a signature proces:

> "Each ElGamal signature or encryption requires a new value of k, and that value must be chosen randomly." (Schneier, p. 477, third paragraph, second sentence).

Claim 1 is respectfully submitted to be allowable for at least the above reasons. Claims 2-5 are dependent on claim 1 and are submitted to be allowable for at least the same reasons.

Claims 6 and 8 also include similar limitations that an encryption and a signature both be determined using the same random number "c". Claims 6 and 8 are respectfully submitted to be allowable. Claim 7 is dependent on claim 6 and is also submitted to be allowable.

IV. Added claims 9-14

Claims 9-14 have been added. Each of claims 9-14 is submitted to have a combination of limitations not shown by the prior art.